

# M-21-31 Compliance: What Government Leaders Need to Know

The Office of Management and Budget's (OMB) M-21-31 provides federal civilian and defense leaders with a much-needed roadmap toward greater cybersecurity.





Public sector leaders face challenging headwinds as near-peer adversaries look to disrupt U.S. operations in cyberspace. As the Department of Defense, the intelligence community and the federal government engage in the next great power competition, the Office of Management and Budget (OMB)'s memorandum [M-21-31](#) sets out a roadmap for enhancing agencies' cybersecurity posture.

"M-21-31 really recognizes the importance of accessible data from the environment that we're looking to protect, and the necessity of broad asset visibility to unlock the intelligence needed to drive effective detection of malicious activity and behaviors in the environment so they can effectively respond to those threats," said Michael Loefflad, senior director for federal systems engineering at SentinelOne.

While the OMB's memorandum builds on [Executive Order \(EO\) 14028 on Improving the Nation's Cybersecurity](#) and precedes the recently updated [National Cybersecurity Strategy](#), the three work in concert to advance cybersecurity at the national level.

Compared to high-level strategy documents like the National Cybersecurity Strategy, M-21-31 delves deeper into the technicalities of what it will take for agencies to enhance cybersecurity within their environments. M-21-31 provides leaders with an easy-to-follow roadmap and defines how agencies can effectively collect, store, and leverage event logs — [files that contain records of events, system messages and user activity](#) — to derive insights at speed and scale.

"M-21-31 is really well done. It lays out a roadmap with timelines and a maturity scale for achieving not just

compliance to the requirements in the mandate, but enhancing the cybersecurity protections that our agencies are deploying in their environments," Loefflad said. "M-21-31 is laying the foundation for collecting and centralizing the right data, making it easily accessible, and driving the data analytics needed to combat fast-moving threat actors in the market today."

Outsmarting these fast-moving threat actors is becoming increasingly important for public sector leaders looking to protect their data, devices and networks from malicious attacks that, according to a 2022 [report from SentinelOne](#), seek to "neutralize and sidestep EDR tools."

Government agencies must evolve faster than these threat actors, and M-21-31's guidelines suggest that enhanced visibility and next-generation capabilities like artificial intelligence (AI), machine learning (ML) and cloud computing could help federal agencies effectively fight back.

### **M-21-31'S Requirements and the Challenges Agencies Face**

Government agencies are working hard to comply with M-21-31. Challenges, however, still exist for a large number of agencies. For example, Loefflad explained that as the government collects more information from an ever-growing number of sources, legacy infrastructure within the federal government will struggle to keep pace.

"When agencies look at that increase in data volume and longer-term retention, they also match it up with incumbent solutions that are in place to do the log storage and analysis," Loefflad said. "What they're finding in



many cases is the technology can't scale, or it can't scale affordably to be able to accommodate that huge volume they're starting to see."

With IT modernization initiatives, numerous agencies are opting to transfer workloads to the cloud to resolve problems caused by outdated infrastructure, but this approach may also result in new complications. If federal agencies fail to formulate a strong cloud security strategy before migration, cloud computing could give rise to siloed or duplicate data stores, lack of full estate-wide visibility, and increased exposures and security risks despite its advantages.

As public sector organizations improve their cybersecurity posture, addressing issues of scale and duplication will be an important task. M-21-31's "Maturity Model for Event Log (EL) Management," implicitly suggests that federal agencies must work toward addressing these longstanding issues to improve visibility into and across their datasets.

For example, federal civilian agencies looking to move from EL1 to EL3 compliance should retain "data or metadata from their environment" and "logs should be centrally aggregated by an agency component-level Enterprise Log Manager (ELM)." In essence, public sector leaders require solutions that scale to support all the data in their environment and that information should be centralized within an ELM for comprehensive security analysis.

Consolidating an organization's event logging data into an ELM may seem like a straightforward task on paper, but in reality, it can be complex and time-consuming. It often takes several months of thorough review to ensure that all relevant data has been collected and integrated into the ELM. Establishing a platform that normalizes various sources of data, provides a method of quickly querying or searching the data, includes autonomous analytics, and is flexible to evolve with the IT environment and threat actor dynamics is critical to achieving the desired outcomes from M-21-31.

Moreover, competing requests and limited resources can further complicate the process. To overcome these obstacles, Loefflad recommended leveraging the power of partnerships and considering new modern data storage and analytics platforms. By partnering with external organizations, like Presidio Federal and SentinelOne, federal leaders can tap into their expertise and resources to accelerate new technology modernization and compliance efforts.

### New Approaches to an Age-Old Problem

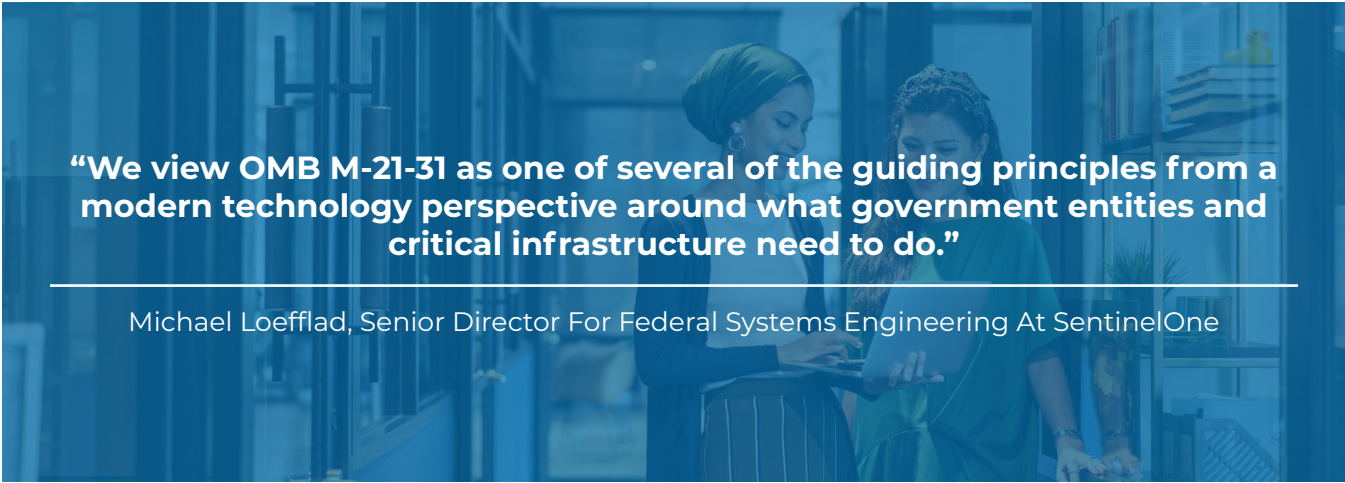
As public and private sector leaders work toward M-21-31 compliance, cloud computing will play a role in helping organizations scale to meet demand. Most federal and defense agencies understand the importance of cloud computing. A report from the Government Accountability Office (GAO) states, "agencies have increased usage [of cloud computing] and realized benefits," but many challenges still remain.

With leaders moving workloads to the cloud, traditional security measures will need to evolve alongside infrastructure. M-21-31 offers agencies a roadmap as to how leaders can effectively manage and extract insights from the cloud telemetry and log data needed to secure their workloads via a cloud-smart approach. Full workload protection and real-time data visibility including virtual machines, applications, containers, and Kubernetes environments deployed on private and public networks is a requirement in this perpetually changing cyber landscape.

Yet many federal, defense and intelligence agencies still rely on manual processes and legacy systems. As the threat landscape evolves, public sector organizations must adopt contemporary technologies and solutions. Automated log management solutions can help security analysts quickly detect, investigate and remediate potential threats faster, shortening the time to containment and freeing employees up to focus on [disrupting and disabling threat actors](#).

**"When agencies look at that increase in data volume and longer-term retention, they also match it up with incumbent solutions that are in place to do the log storage and analysis. What they're finding in many cases is the technology can't scale, or it can't scale affordably to be able to accommodate that huge volume they're starting to see."**

Michael Loefflad, Senior Director For Federal Systems Engineering At SentinelOne



**“We view OMB M-21-31 as one of several of the guiding principles from a modern technology perspective around what government entities and critical infrastructure need to do.”**

Michael Loefflad, Senior Director For Federal Systems Engineering At SentinelOne

“We have the solution to secure cloud workloads and provide the same level of autonomous security and protection that we provide to a traditional endpoint,” Loefflad said. “We can extend the same AI-driven protections, data and log consolidation and retention, and autonomous security analytics capabilities to the cloud workloads that they’re deploying.”

While M-21-31 does not explicitly mention the use of AI in cybersecurity, Loefflad and other industry experts highly recommend that agencies leverage the technology to enhance and support a more robust cybersecurity posture.

“Agencies can leverage AI technologies to autonomously assess activities, behaviors happening on IT assets and really drive assessments of those activities to determine malicious and suspicious behavior,” Loefflad said. “That way, we can trigger real-time protection, detection and response actions against those activities in the environment.”

Monitoring user and application behaviors within cloud workloads and on agency endpoints can be difficult, but it doesn’t have to be. AI/ML can help make it easier for security operations center (SOC) analysts to get a handle on their workloads, and when needed, respond quickly to any emerging threats.

For example, Loefflad pointed out that generative AI (GAI) and natural language processing could be used to simplify complex queries or programming languages. Instead of needing to know complex or proprietary query syntax, SOC analysts could ask the application a question in a natural way and receive a natural language response back.

This streamlined approach to investigation can help drive efficiencies in day-to-day threat research, helping overworked analysts quickly parse the threat data coming into the SOC.

Responding to these emerging threats is no easy task and requires government leaders to leverage next-generation capabilities. M-21-31 acknowledges this unspoken requirement and provides agencies with the roadmap to enhance their cybersecurity posture, starting with increased visibility from proper event log management and faster response powered by applied AI/ML analytics.

“We view OMB M-21-31 as one of several of the guiding principles from a modern technology perspective around what government entities and critical infrastructure need to do,” Loefflad said.

**Discover how SentinelOne and Presidio Federal can help your agency advance M-21-31 compliance.**